UNITED STATES DISTRICT COURT
DISTRICT OF PUERTO RICO

UNITED STATES OF AMERICA,
Plaintiff,

v. **Civil Action No. 25-mc-00068-FAB**

JUAN CARLOS REYNOSO,
Defendant.

DECLARATION OF SPECIAL AGENT ALEX SANTIAGO-MONTES IN SUPPORT OF GOVERNMENT'S OPPOSITION TO DEFENDANT'S AMENDED MOTION TO QUASH SERVICE OF SEIZURE WARRANT

I, Alex Santiago-Montes, declare as follows:

1. I am a Special Agent with the Federal Bureau of Investigation in San Juan, Puerto Rico. I make this declaration in support of the United States of America's Opposition to Defendant's Amended Motion to Quash Service of a Seizure Warrant. I make this declaration of my own personal knowledge or on information and belief where noted. If called as a witness, I could and would testify completely to the truth of the matters set forth herein.
2. I have been a Special Agent with the FBI since 2020. My primary responsibility has been to investigate fraud involving federal health care programs and Financial Crimes including bank fraud, wire fraud, Ponzi schemes, embezzlements, and other types of fraud schemes as well as schemes related to cyber-crimes. Prior to this, I worked as a Financial Operations Specialist with the FBI for approximately 5 years. I also worked as a Validation Specialist for Fluor Daniel Caribbean Inc. at different pharmaceutical projects. I have received extensive training at the Basic Training Program at the FBI Academy in Quantico. I have a Bachelor's Degree in Chemical Engineering and a Master's Degree in Engineering Management from the Polytechnic University

of Puerto Rico.

3. Based on my training and experience, I am familiar with the following concepts related to cryptocurrency:

   a. *Bitcoin* (or "BTC") is a type of virtual currency. Unlike traditional, government-controlled currencies (*i.e.*, fiat currencies), such as the U.S. dollar, Bitcoin is not managed or distributed by a centralized bank or entity. Because of that, Bitcoin can be traded without the need for intermediaries. Bitcoin transactions are approved/verified by computers running Bitcoin's software. Those computers are called network nodes. Each node uses cryptography to record every Bitcoin transaction on the Bitcoin blockchain. The Bitcoin blockchain is a public, immutable, distributed ledger.

   b. Each Bitcoin account is divided into distinct *unspent transaction outputs* ("UTXOs"). When a person initiates a transaction, they must use an entire UTXO—there is no mechanism to spend only a fraction of it. I f the amount being sent is less than the full UTXO, the remainder (or "change") is returned to the sender in the same transaction. Although it may appear that the user is spending everything in their wallet, in actuality the unused portion is automatically sent back to them. This is similar to fiat currency in the following manner: If someone has a single $100 bill and wants to purchase a $30 item, he must hand over the entire $100 bill to the cashier. The cashier then gives $70 back as change. Bitcoin works in a similar way. If a user has one UTXO worth 1 Bitcoin (comparable to the $100 bill) but wants to send only 0.3 Bitcoin (comparable to the $30 bill), he must use the entire 1 Bitcoin in the transaction. The recipient gets the 0.3 Bitcoin, and the remaining 0.7 Bitcoin is sent to an address other than the recipient's.

   c. In blockchain-analysis, there is a *"round-number heuristic*" (sometimes also referred to as a "round-payment heuristic") that classifies outputs in a transaction based on

whether they look like a whole number (*e.g.* exactly 1.0 BTC, 2.0 BTC, etc.) or an odd decimal. Under this heuristic:

i. The "round" (whole-number) output is presumed to be the intended payment (the spender's actual send), and

ii. The "non-round" (odd decimal) output is presumed to be change sent to a wallet controlled by the sender.

d. An example will help to clarify: Alice has 2.35 BTC in her wallet and needs to pay Bob exactly 1.0 BTC. She creates a transaction that draws the entire 2.35 BTC from her address (because she must transfer all of the Bitcoin out of the wallet), and she then sends 1.0 BTC to Bob's address and 1.3499 BTC to a wallet that she controls as "change" (with a small deduction for transaction fees). When this transaction appears on the blockchain, analysts see two outputs: one is 1.0 BTC, the other 1.3499 BTC. Because 1.0 BTC is a whole number, one can reasonably infer in most instances that it is the intended payment to Bob. Meanwhile, the non-round 1.3499 BTC output typically would be the change being sent to a wallet under Alice's control.

e. A *private key* is a cryptographic key that is uniquely associated with an entity. It is not made public. In the blockchain and virtual currency context, a private key (which is like a password) controls a virtual currency address or addresses. The private key is needed to access the funds associated with the address. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address.

f. In order to store their keys, users have *virtual currency wallets*. These wallets store a user's keys, allowing a user to send and receive virtual currency stored on the blockchain. A *virtual currency address* is an alphanumeric string that designates the virtual location

on a blockchain where virtual currency can be sent and received. A virtual currency wallet can store multiple virtual currency addresses.

g. One type of virtual currency wallet is a *hardware wallet*. A hardware wallet is a physical\device that stores a user's private keys and can be connected to a computer when a user wishes to use the keys stored on the wallet for virtual currency transactions. Hardware wallets can be secured with PINs and passphrases and can be backed up or regenerated with a recovery phrase.

h. A hardware wallet helps to ensure that only the person who is in physical possession of the hardware wallet (and therefore has access to the private keys stored on that wallet) can transfer funds from the associated virtual currency address(es).

i. There are various brands of hardware wallet, including "Ledger." Below is a screenshot describing Ledger's hardware wallet from https://shop.ledger.com/pages/hardware-wallet:

What is a hardware wallet?

A hardware wallet is a physical device that stores your private keys on a Secure Element. The Secure Element also drives the device's screen to ensure that a transaction can't be tampered with.

When you want to clear sign a transaction, the Ledger Secure OS decodes the transaction details and displays it in a human-readable format so that you know what you're signing.

How do hardware wallets work?

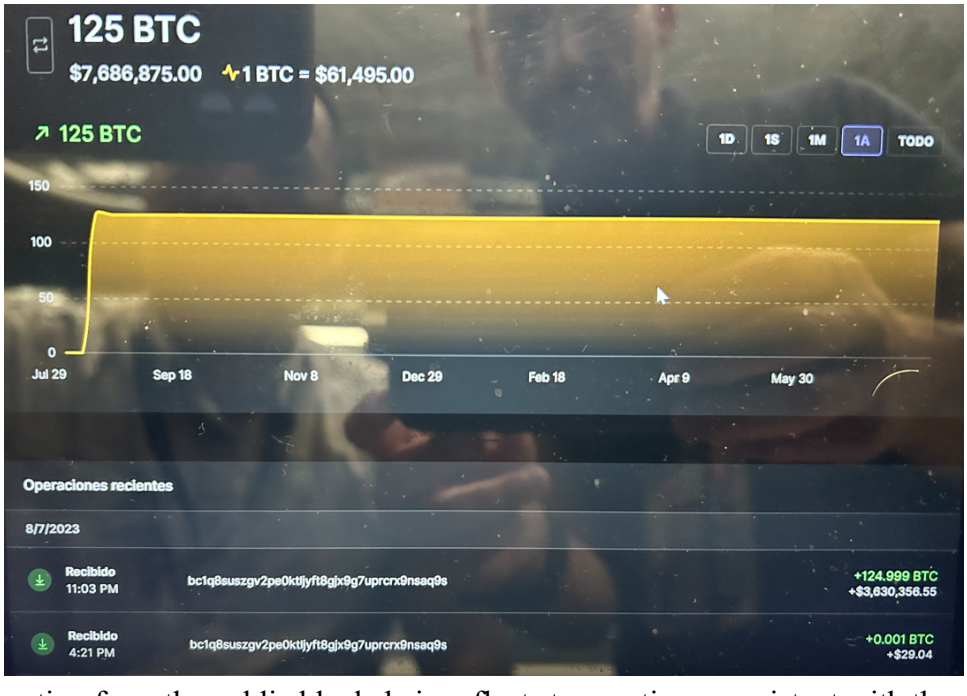
Hardware wallets use Secure Element chips that are also used for credit cards and passports. The chip generates and stores your private keys and prevents physical attacks. Hardware wallets also contain an operating system (OS) that is responsible for running the apps. When setting up your hardware wallet, you'll have to set your PIN code and write down your seed phrase. Then you can sign or reject transactions with your hardware wallet.

Why Do Private Keys Matter?

Private keys are unique strings of letters and numbers that allow you to access your digital assets. Cryptocurrencies are not stored within the crypto wallet itself but on the blockchain. Private keys are crucial to the security and ownership of your crypto, as they are the only way to prove that you are the rightful owner of your digital assets. Therefore, your private keys must be kept secret and secure at all times. Hardware wallets provide a secure way to store and manage your private keys, keeping them offline and out of reach of online threats.

4. Pursuant to a federal search warrant executed on June 30, 2024, the FBI seized from Mr. Reynoso electronic equipment, including Apple devices, a Lenovo laptop computer, and a Ledger hardware wallet.

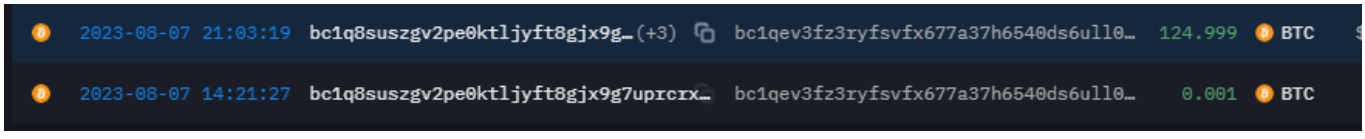
5. The Lenovo laptop seized from Mr. Reynoso contained software for the Ledger hardware wallet that reflected the wallet's cryptocurrency balances as of the last login session. Specifically, the software homepage reflected an incoming transaction ("received") of approximately 125 BTC from address bc1q8suszgv2pe0ktljyft8gjx9g7uprcrx9nsaq9s (hereinafter "**bc1q8s**") on August 7, 2023 at 11:03 PM. A screenshot of that homepage from the laptop seized from Mr. Reynoso is below:



6. Information from the public blockchain reflects transactions consistent with those shown in the above screenshot. In particular, the blockchain indicates that address **bc1q8s** sent the following transfers:

a. 124.999 BTC on August 7, 2023 at 9:03 PM to address bc1qev3fz3ryfsvfx677a37h6540ds6ull0sap6drv (hereinafter "**bc1qev**")[1]
b. 0.001 BTC on August 7, 2023 at 2:21 PM to **bc1qev**.

A screenshot from the website intel.arkm.com, which reflects the above transactions, is below:



7. The details of these transaction and their ties to Reynoso were corroborated by a text file located on Reynoso's Apple account, which depicted the above transactions. A screenshot of this note is below:[2]

[1] The screenshot of the Ledger software reflects a time of 11:03 PM on August 7, 2023 for the transfer of 124.999 BTC. The public blockchain data, as made available through the website intel.arkm.com, reflects a time of 9:03 PM on August 7, 2023 for the transfer of 124.999 BTC. There is what appears to be an identical two-hour difference for the transaction of 0.001 BTC. However, these differences can be attributed to the use of distinct time zones. Given the global nature of Bitcoin, it is not uncommon for transactions to be reflected in different time zones.

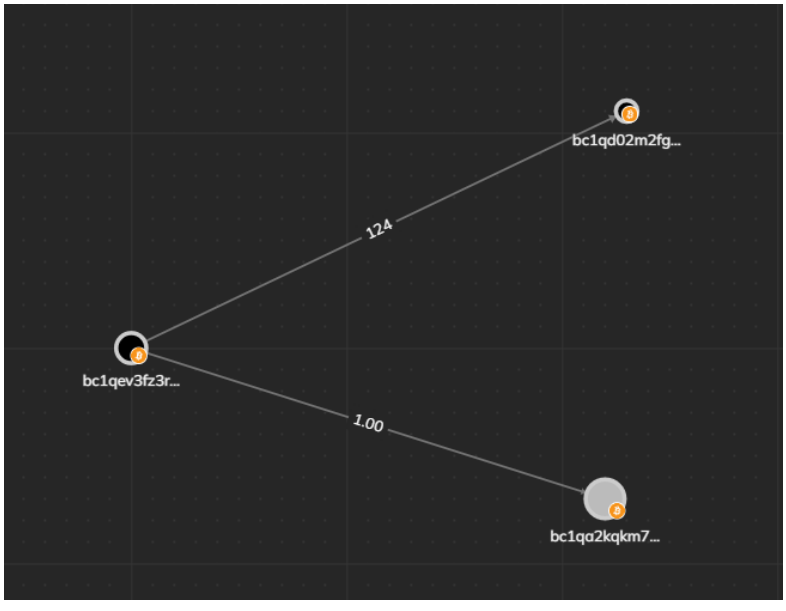
[2] The "Transaction History" receipt from Ledger has the same dates but different times than the transactions recorded on the blockchain. Bitcoin transactions can take minutes to hours to be confirmed on the public blockchain. Ledger's website states that, after someone has sent Bitcoin from an account in Ledger, "[i]t takes some time for the transactions to get confirmed on the blockchain and depending on the fees you selected, it may take from 1 minute to several hours." https://support.ledger.com/article/9498747905181-zd. Consequently, the times reflected on the Ledger receipt would be earlier than the times for a confirmed transaction on the blockchain.

8. At the bottom right corner of the above note, there is a reference to "Ledger." According to Ledger's website, users can export their cryptocurrency transaction history as files. *See https://support.ledger.com/article/360014094879-zd* ("You can export your operation/transaction history in the Ledger Live desktop app as a CSV file.").

9. Based on the information recorded publicly on the blockchain, on or about January 29, 2025, the address **bc1qev** sent 123.999 BTC to the address bc1qd02m2fgh82dcefymtpq3mxxqvydz29rfcgdgac (**bc1qd0**) and 1 BTC to the address bc1qa2kqkm7fwzr8s0jtfrn8ggsg6g4nuql8esghnz (**bc1qa2**). A depiction of those transactions, based on information recorded publicly on the blockchain, is below:

Date	Transaction Hash	From	To	BTC Amount	USD Amount
1/29/2025	5316e2292019c12d17fe29a8c	bc1qev3fz3ryfsvfx677a37h	bc1qa2kqkm7fwzr8s0jtfrn8ggsg6g4nuql8esghnz	1	$ 101,862.30
	83880393edcc3bee0e45dd075	6540ds6ull0sap6drv	bc1qd02m2fgh82dcefymtpq3mxxqvydz29rfcgdgac	123.9999938	$ 12,630,924.57

A graphic representation (rounding to the nearest whole number) of the outflow of funds from address **bc1qev** on January 29, 2025 is below:



10. In the Bitcoin network, when a person initiates a transaction from a Bitcoin address (such as address bc1qev), they must spend the entire amount of Bitcoin in that address, even if those amounts are sent to different addresses (such as address bc1qa2 and address bc1qd0). Consequently, if Mr. Reynoso were transferring Bitcoin from address bc1qev, he would need to send the entirety of this amount to one or more addresses.

11. A document, dated March 6, 2024, located on Reynoso's Apple account indicated that Reynoso controls the address **bc1qa2**. In particular, "Juan Carlos Reynoso" signed a letter in which he stated "I am the owner of the wallet provided for the transfer. bc1qa2kqkm7fwzr8s0jtfrn8ggsg6g4nuql8esghnz." This document is attached at Exhibit A-1.

12. Based on the *round-number heuristic* described, above, in paragraph 3(c), the non-round number, 123.999 BTC, sent to address bc1qd0 would be "change" transferred to a successor wallet under the control of Mr. Reynoso. Address bc1qd0 was the subject of the Seizure Warrant. In addition,

the round number, 1 BTC, was sent to address bc1qa2, which, as described in the preceding paragraph, is also under Mr. Reynoso's control.

13. Furthermore, based on information recorded publicly on the blockchain, the only transactions to/from address **bc1qev** were the incoming transactions of August 7, 2023 described above and the outgoing transaction of January 29, 2025 described above. A chart of all transactions to/from address **bc1qev** is reproduced below from intel.arkm.com:

TRANSFERS		INFLOW	OUTFLOW	
TIME	FROM	TO	VALUE	TOKEN
2025-01-29 16:23:01	bc1qev3fz3ryfsvfx677a37h6540ds6ull0…	bc1qd02m2fgh82dcefymtpq3mxxqvyd… (+1)	125	BTC
2023-08-07 21:03:19	bc1q8suszgv2pe0ktljyft8gjx9g7up… (+3)	bc1qev3fz3ryfsvfx677a37h6540ds6ull0…	124.999	BTC
2023-08-07 14:21:27	bc1q8suszgv2pe0ktljyft8gjx9g7uprcrx…	bc1qev3fz3ryfsvfx677a37h6540ds6ull0…	0.001	BTC

I declare under penalty of perjury under the law of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed on February 28, 2025 in San Juan, Puerto Rico.

Special Agent Alex Santiago-Montes
Federal Bureau of Investigation